



November is Critical Infrastructure Security and Resilience Month, an opportunity to highlight the efforts between Federal, State, local, territorial, and tribal governments and private sector partners to protect and secure our Nation's critical infrastructure and enhance infrastructure resilience.

### What Critical Infrastructure Means To You

The Nation's critical infrastructure provides essential services that underpin American society and sustain the American way of life. We know critical infrastructure as the power we use in our homes and businesses, the water we drink, the transportation systems that get us from place to place, the first responders and hospitals in our communities, the farms that grow and raise our food, the stores we shop in, and the Internet and communication systems we rely on to stay in touch with friends and family.

Protecting and promoting the continuity of our Nation's critical infrastructure is essential to our security, public health and safety, and economic vitality. Through a series of initiatives, Critical Infrastructure Security and Resilience Month reinforces the importance of critical infrastructure to America's homeland security and economic prosperity and reiterates the Department's commitment to keep our critical infrastructure, and the communities that depend on them, safe and secure. This requires a nationwide effort, with public and private partners working together toward a common goal.



This year, Critical Infrastructure Security and Resilience Month activities will focus on several key areas to enhance security and resilience:

- Highlighting interdependencies between cyber and physical infrastructure.
- Pointing small and medium-sized businesses to the free tools and resources available to them to increase their security and resilience through Hometown Security and the four steps of Connect, Plan, Train, and Report ([www.dhs.gov/hometown-security](http://www.dhs.gov/hometown-security)).
- Promoting public-private partnerships.
- Fostering innovation and investments in infrastructure resilience.

### Risks to Critical Infrastructure

Critical infrastructure is increasingly at risk from a variety of risks, both natural and man-made, that continue to evolve—including climate change, extreme weather, aging and failing infrastructure components, cyberattacks, pandemics, and acts of terrorism. In particular, physical and cyber infrastructure have grown inextricably linked, meaning both cyber and physical measures are required to guard against the full array of threats. Growing interdependencies among infrastructure sectors and lifeline functions also impact the management of infrastructure risk. Understanding and mitigating these risks is a key element of our national security, resilience, and economic prosperity.

## The Role of DHS

The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) leads the coordinated national effort to manage risks to our Nation's critical infrastructure. NPPD leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. IP focuses on protecting critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

The Department leads this national effort by working with critical infrastructure partners to achieve the aims articulated in the [National Infrastructure Protection Plan \(NIPP\)](#). The NIPP envisions critical infrastructure that is secure and able to withstand and rapidly recover from all hazards. It focuses on a set of lifeline functions—communications, energy, transportation, and water management—to support preparedness and continuity of operations.

## How You Can Get Involved

- Visit [www.dhs.gov/cisr-month](http://www.dhs.gov/cisr-month) to get more information.
- Share stories and information about your efforts in support of infrastructure security and resilience with your customers, constituents, partners, residents, and employees through newsletters, websites, emails, blog posts, and tweets.
- Reinforce the role your organization or office plays in infrastructure security and resilience by incorporating references to Critical Infrastructure Security and Resilience Month in speaking engagements and events.
- Follow [@DHSgov](#) on Twitter or [Department of Homeland Security](#) on Facebook, and post infrastructure security and resilience efforts, tips, news, and resources on social media sites using **#infrastructure**.
- Request a Critical Infrastructure Security and Resilience Month Toolkit to help spread the word by visiting [www.dhs.gov/cisr-month](http://www.dhs.gov/cisr-month) or emailing [infrastructure@hq.dhs.gov](mailto:infrastructure@hq.dhs.gov).

Americans can do their part at home, at work, and in their local communities by being prepared for all hazards, reporting suspicious activities, and learning more about critical infrastructure security and resilience.

## The Critical Role of Partnerships

Securing critical infrastructure and ensuring its resilience is a shared responsibility of Federal, State, local, tribal, territorial, and private sector partners, as well as individual citizens. Just as we all rely on critical infrastructure, we must all play an active role in keeping it strong, secure, and resilient. To this end, the Department works with Federal, State, local, tribal, and territorial agencies and the private sector to address critical infrastructure national security imperatives to secure vital assets, ensure continuity of operations, and prepare for response to and recovery from all hazards.

Public-private partnerships, in particular, are vital to this effort. Because the majority of our national critical infrastructure is owned and operated by private companies, both the government and private sector have a common incentive to reduce the risks of disruptions to critical infrastructure. Strengthening public-private partnerships focused on critical infrastructure protection is both a national security and business imperative.

- **Information Sharing:** DHS facilitates information sharing across infrastructure stakeholders. This includes sharing sensitive information regarding critical infrastructure, threats, and best practices to strengthen owners' and operators' decision-making capabilities.
- **Training and Education:** DHS facilitates collaborative exercises and provides training materials, courses, and consultation to sector partners across the Nation and internationally, augmenting the critical infrastructure community's awareness, preparedness, and response capabilities.
- **Partnerships:** DHS facilitates partnerships across Federal, State, local, tribal, and territorial entities and the private sector that enable comprehensive response and collaborative engagement throughout the critical infrastructure community.
- **Assessments, Analysis, and Regulatory Compliance:** DHS supports critical infrastructure partners in achieving regulatory compliance and managing risk based on threat, vulnerability, and potential consequence assessments. Risk assessments and analysis helps identify requirements for security programs and resiliency strategies.